REMARKS:

In the Office Action the Examiner noted that claims 1-4, 6-24 and 26-41 are pending in the application, and the Examiner rejected all claims.

By this Amendment, claims 1, 7, 20, 21, 27, 40 and 41 have been amended. No new matter has been presented. Claims 5 and 25 remain cancelled. Thus, claims 1-4, 6-24 and 26-41 are pending in the application. The Examiner's rejections are traversed below, and reconsideration of all rejected claims is respectfully requested.

CLAIM REJECTIONS UNDER 35 USC § 102:

On page 3 of the Office Action the Examiner rejected claims 1-4, 6-24 and 26-41 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,987,557(Ebrahim). Applicants respectfully traverse the Examiner's rejections of the remaining claims.

The Examiner maintains that Ebrahim each and every element of the independent claims. Applicants respectfully disagree with this assertion for at least the following reasons.

Ebrahim discusses enabling access based on an access-match signal resulting from a comparison of transaction path signals carried by at least a subset of the physical address signal lines and an access signal line to signals from the storage designating the protection domains and accessibility of the protection domains.

On the other hand, claim 1 recites, "a storing unit that is loaded on the hardware secure module and stores an updated secure software in an unswappable area of the memory using a direct access method", where the storing unit instructs, using the direct access method, the processor to change over from the secure software executed to the updated secure software stored in the unswappable area of the memory and to execute the updated secure software." The Applicants respectfully submit that Ebrahim does not disclose or suggest at least this feature of claim 1.

Ebrahim explicitly states:

> "...operations of the protection check logic block 300 are indistinguishable whether the processor is executing a privileged instruction or executing in a supervisor mode...only privileged software, such as operating system kernel, may cause the supervisor (S) signal to become asserted...the context signal includes a plurality N of context bits from a context register 310 that designates the context number of the currently running process..."

(column 8, lines 6 to 29 of Ebrahim).

As mentioned above, Ebrahim merely discusses that operations of logic block are indistinguishable whether the processor is executing a privileged instruction or executing in a supervisor mode. However, Ebrahim is silent regarding storing "an updated secure software in an unswappable area of the memory using a direct access method" and instructing "using the direct access method, the processor to change over from the secure software executed to the updated secure software stored in the unswappable area of the memory and to execute the updated secure software", as recited in claim 1. See also other independent claims reciting similar features. Hence, each feature of independent claims is patentably distinguishable over Ebrahim and independent claims are patentable.

Therefore, since Ebrahim does not disclose the features recited in the independent claims, as stated above, it is respectfully submitted that claims patentably distinguishes over Ebrahim, and withdrawal of the §102 rejection is earnestly and respectfully solicited.

Claims depending from the independent claims include all of the features of that claim plus additional features which are not disclosed by Ebrahim. For at least the same reasons, claims depending from the independent claims are also patentably distinguishable over Ebrahim.

Therefore, withdrawal of the rejection is respectfully requested.

CLAIM REJECTIONS UNDER 35 USC §103:

On page 6 of the Office Action the Examiner rejected claims 13-18, and 33-38 under 35 U.S.C. § 103(a) as being unpatentable over Ebrahim in view of U.S. Patent No. 5,022,077 (Bealkowski).

Bealkowski does not add anything to the teachings of Ebrahim with respect to the claimed invention. Further, as Bealkowski merely discusses a protected region that has a BIOS image loaded into a memory and activated using the operating system, Bealkowski does not cure the deficiencies of Ebrahim regarding claims of the present application.

The Examiner maintains that the combination of Ebrahim and Bealkowski would be obvious in order to allow authorized system to boot up BIOS image as taught by Bealkowski. Applicants respectfully submit that there a reason for a particular combination of Ebrahim and Bealkowski has not been provided to establish obviousness (see, *KSR International Co. v. Tele-flex Inc. (KSR)*, 82 USPQ2d 1385 (2007)). In this case, the rejection based on Ebrahim and Bealkowski is made by mere conclusory statements. Essentially, the Action concludes that the

combination would have been obvious "in order to allow authorized system to boot up BIOS image as taught by Bealkowski."

Applicants request that some reasoning with some rational underpinning be provided to support the legal conclusion of obviousness since absent improper hindsight the record, however, fails to provide the required evidence (rationale) of a motivation for a person of ordinary skill in the art to perform such modification.

Moreover, even if Ebrahim and Bealkowski are combined, the combination does not teach or suggest the claimed invention. For example, claim 17 recites, "a writing unit that is loaded in the hardware secure module, wherein the writing unit writes a secret information within the hardware secure module into the memory using the direct access method", where falsification is checked based on "response information corresponding to the secret information." Ebrahim and Bealkowski do not teach or suggest modified information and falsification checking based on the information.

Therefore, withdrawal of the rejection is respectfully requested.

CONCLUSION:

There being no further outstanding objections or rejections, it is respectfully submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 04/07/2011

By: Temnit Afework

1201 New York Ave, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

Temnit Afework
Registration No. 58,202